LISTING OF CLAIMS

1-44. (Cancel)

45. (**New**) A method in a data packet receiving path of a system, comprising:

receiving a incoming encoded data packet at a lower layer of the system;

determining whether the lower layer of the system has cryptography information cached with which to perform cryptography operations on the data packet, and if so, processing the data packet in hardware;

if the lower layer of the system does not have cryptography information cached with which to perform the cryptography operations on the data packet, indicating the data packet to an upper layer of the system; and

passing the cryptography information with which to perform the cryptography operations on the data packet from the upper layer to the lower layer to enable the lower layer to cache the cryptography information for use with subsequent cryptography operations associated with transmit or receipt of a subsequent data packet.

46. (**New**) The method of claim 45, wherein the upper layer comprises an intermediate driver agent.

47. (**New**) The method of claim 45, wherein the lower layer comprises base driver agent.

48. (**New**) The method of claim 45, wherein the cryptography information comprises at least one of a unique identifier, a network protocol associated with the data packet, a security parameter index, a cryptographic key, a source identifier, or a destination identifier.

49. (**New**) The method of claim 45, further comprising:

the upper layer of the system re-submitting the data packet to the lower layer to perform hardware offload of the cryptography operations to the lower layer.

50. (**New**) The method of claim 45, wherein passing the cryptography information from the upper layer to the lower layer comprises:

passing a pointer from the upper layer to the lower layer that points to a data structure including the cryptography information.

51. (**New**) The method of claim 50, further comprising:

the lower layer accessing the cryptography information in the data structure to populate a cryptography information table stored at the lower layer.

52. (**New**) An article comprising a storage medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

receive a incoming encoded data packet at a lower layer of the system;

determine whether the lower layer of the system has cryptography information cached with which to perform cryptography operations on the data packet, and if so, process the data packet in hardware;

if the lower layer of the system does not have cryptography information cached with which to perform the cryptography operations on the data packet, indicate the data packet to an upper layer of the system; and

pass the cryptography information with which to perform the cryptography operations on the data packet from the upper layer to the lower layer to enable the lower layer to cache the cryptography information for use with subsequent cryptography operations associated with transmit or receipt of a subsequent data packet.

53. (**New**) The article of manufacture of claim 52, wherein the upper layer comprises an intermediate driver agent.

54. (**New**) The article of manufacture of claim 52, wherein the lower layer comprises base driver agent.

55. (**New**) The article of manufacture of claim 52, wherein the cryptography information comprises at least one of a unique identifier, a network protocol associated with the data packet, a security parameter index, a cryptographic key, a source identifier, or a destination identifier.

56. (**New**) The article of manufacture of claim 52, further comprising instructions to:

re-submit the data packet from the upper layer to the lower layer to perform hardware offload of the cryptography operations to the lower layer.

57. (**New**) The article of manufacture of claim 52, wherein the instructions to pass the cryptography information from the upper layer to the lower layer comprise instructions to:

pass a pointer from the upper layer to the lower layer that points to a data structure including the cryptography information.

58. (**New**) The article of manufacture of claim 57, further comprising instructions to:

accessing the cryptography information in the data structure with the lower layer to populate a cryptography information table stored at the lower layer.

59. (**New**) An apparatus comprising:

a network interface card to receiving an encoded data packet from a network;

a base driver agent coupled to the network interface card to determine if the network interface card includes cryptography information cached on a memory on the network interface card with which to perform cryptography operations on the data packet, and if so, process the data packet in hardware, and if not, indicate the data packet to an upper layer driver; and

an upper layer driver coupled to the base driver agent to receive the indication of the data packet from the base driver agent, and pass the cryptography information with which to perform the cryptography operations on the data packet to the base driver agent to enable the base driver agent to cache the cryptography information on the network interface card for use with subsequent cryptography operations associated with transmit or receipt of a subsequent data packet.

60. (**New**) The apparatus of claim 59, wherein the cryptography information comprises at least one of a unique identifier, a network protocol associated with the data packet, a security parameter index, a cryptographic key, a source identifier, or a destination identifier.

61. **(New)** The apparatus of claim 59, the upper layer driver to further:

re-submit the data packet to the base driver agent to perform hardware offload of the cryptography operations to the network interface card.

62. **(New)** The apparatus of claim 59, the upper layer driver to pass the cryptography information to the base driver agent further comprising:

the upper layer driver to pass a pointer to the base driver agent that points to a data structure including the cryptography information.

63. **(New)** The apparatus of claim 62, the base driver agent to further:

access the cryptography information in the data structure to populate a cryptography information table stored on the network interface card.

64. **(New)** A method in a data packet transmit path of a system, comprising:

associating cryptography information with a data packet at an upper layer of the system, the cryptography information to provide all information necessary to encode the data packet, the system including cryptography information caching;

passing the cryptography information with the data packet from the upper layer to a lower layer of the system, regardless of whether or not the lower layer already has the cryptography information cached;

performing cryptography operations on the data packet; and

if the lower layer does not already have the cryptography information cached, caching the cryptography information at the lower layer for use with subsequent cryptography operations associated with transmit or receipt of a subsequent data packet.

65. **(New)** The method of claim 64, wherein the upper layer comprises an intermediate driver agent.

66. **(New)** The method of claim 64, wherein the lower layer comprises base driver agent.

67. **(New)** The method of claim 64, wherein the cryptography information comprises at least one of a unique identifier, a network protocol associated with the data packet, a security parameter index, a cryptographic key, a source identifier, or a destination identifier.

68. **(New)** The method of claim 64, wherein passing the cryptography information from the upper layer to the lower layer comprises:

passing a pointer from the upper layer to the lower layer that points to a data structure including the cryptography information.

69. **(New)** The method of claim 64, wherein caching the cryptography information at the lower layer further comprises:

accessing the cryptography information in the data structure with the pointer to populate a cryptography information table stored at the lower layer.

70. **(New)** An article comprising a storage medium to provide machine-readable instructions that, when executed, cause one or more electronic systems to:

associate cryptography information with a data packet at an upper layer of the system, the cryptography information to provide all information necessary to encode the data packet, the system including cryptography information caching;

pass the cryptography information with the data packet from the upper layer to a lower layer of the system, regardless of whether or not the lower layer already has the cryptography information cached;

perform cryptography operations on the data packet; and

if the lower layer does not already have the cryptography information cached, cache the cryptography information at the lower layer for use with subsequent cryptography operations associated with transmit or receipt of a subsequent data packet.

71. **(New)** The article of manufacture of claim 70, wherein the upper layer comprises an intermediate driver agent.

72. (**New**) The article of manufacture of claim 70, wherein the lower layer comprises base driver agent.

73. (**New**) The article of manufacture of claim 70, wherein the cryptography information comprises at least one of a unique identifier, a network protocol associated with the data packet, a security parameter index, a cryptographic key, a source identifier, or a destination identifier.

74. (**New**) The article of manufacture of claim 70, further comprising instructions to:

re-submit the data packet from the upper layer to the lower layer to perform hardware offload of the cryptography operations to the lower layer.

75. (**New**) The article of manufacture of claim 70, wherein the instructions to cache the cryptography information at the lower layer further comprise instructions to:

access the cryptography information in the data structure with the pointer to populate a cryptography information table stored at the lower layer.